BAB III
PEMBAHASAN

3.1 Analisa Sistem Jaringan yang sedang digunakan

3.1.1 Spesifikasi Alat

Pada PT Indonesia Power UBP Saguling menggunakan spesifikasi alat perangkat keras tiap komputer seperti berikut yaitu:

1. Perangkat Keras

a. NIC (Network Interface Card)

Adalah sebuah kartu jaringan yang digunakan untuk menghubungkan komputer dengan media transmisi (kabel). Dalam jaringan pada PT Indonesia Power UBP Saguling umumnya NIC yang digunakan adalah NIC yang telah terdapat pada *Motherboard (onboard).*



Gambar 3.1 NIC (Network Interface Card)

b. HUB / Switch

HUB / Switch merupakan suatu alat yang digunakan untuk membagi jaringan.Pada jaringan di Indonesia Power UBP Saguling terdapat beberapa tipe HUB/Switch yaitu:

a. Untuk HUB/Switch yang berada di Gd. Administrasi

- Main Switch (CISCO 4507) 24 port 1000 Mbps Core Switch.
- Main Switch (CISCO 5500) 24 port 10/100 Mbps.
- Switch AT -8026FC 24 port 10/100 Mbps



Gambar 3.2 Main Switch (CISCO 4507)



Gambar 3.3 Main Switch (CISCO 5500)

b. Untuk HUB/Switch yang berada di Gd. Unit 5-7
   - Switch AT -8026FC 24 port 10/100 Mbps
   - Switch AT-8400 24 port 10/100 Mbps

c. Untuk HUB/Switch yang berada di Gd. Batubara
   - Switch AT -8026FC 24 port 10/100 Mbps
   - Switch AT-8400 24 port 10/100 Mbps

d. Untuk HUB/Switch yang berada di Gd. Unit 1-4
   - Switch AT -8026FC 24 port 10/100 Mbps
   - Switch AT-8400 24 port 10/100 Mbps

e. Untuk HUB/Switch yang berada di Gd. Unit 1-4 (Alat Bantu/Gudang)
   - Switch AT -8026FC 24 port 10/100 Mbps
   - Switch AT-8400 24 port 10/100 Mbps

Dalam jaringan di PT Indonesia Power UBP Saguling rata-rata ditiap-tiap gedung menggunakan Switch AT-8026FC untuk membagi jaringan, adapun dalam jaringan tersebut secara keseluruhan terdapat 31 Switch di seluruh gedung.



Gambar 3.4 Switch AT-8206FC



Gambar 3.5 Switch 8400

c. Bandwith Management (Packeteer Xprees 1500)

Pada sistem jaringan di PT Indonesia Power UBP Saguling menggunakan Banwith management yang berfungsi untuk memenej banwith ke setiap jaringan komputer. Adapun alat tersebut yaitu *Packeteer Xprees 1500***.**



Gambar 3.6 *Packeteer Xprees 1500*

d. Router (CISCO Router ISR 2821)

Pada sistem jaringan di PT Indonesia Power UBP Saguling menggunakan Router *CISCO Router ISR 2821***.**



Gambar 3.7 *CISCO Router ISR 2821*

e. Konektor

Pada jaringan PT Indonesia Power terdapat hanya memakai satu koneksi yaitu dengan kabel. Untuk kabel menggunakan kabel UTP dan FO.

f. Kabel

1. UTP

   Untuk UTP yang dipakai oleh PT Indonesia UBP Saguling menggunakan UTP kategori 5. Panjang maksimal satu utas kabel LAN adalah 100 meter, bila panjang yang dibutuhkan adalah lebih dari 100 meter, maka dapat digunakan switch untuk menyambung kabel berikutnya. Dengan kabel UTP category 5 dapat mentransmisi data sampai dengan 100Mbps.

2. FO

   Jarak dari unit ke unit PT Indonesia Power UBP Saguling lumayan jauh maka dari itu dipakailah kabel *FO Maximum data* yang dapat ditransmisikan melebihi 1000 Gbits persecond tanpa menggunakan *repeater*.

g. Server

Pada PT Indonesia Power UBP Saguling server yang digunakan adalah produk dari IBM type SERIE 3650 dengan spesifikasi sebagai berikut:

1. Processor Xeon 3 Ghz
2. Memori DDR 2 GB
3. HDD 1 TB
4. Dual 10/100/1000 Ethernet
5. PXE and On LAN
6. CDROM
7. Support Full Duplex
8. 351W Auto Switch PS with ASR

h. Komputer *Client*

Pada dasarnya semua PC yang berada pada PT. Indonesia Power UBP Saguling memiliki cirri dan spesifikasi yang sama karena sistem pengadaan komputer secara merata kepada setiap *user/*. Adapun spesifikasi komputer adalah:

1. Intel Pentium Processor P4 2,2 GHz 1.2 Cache 2MB, FSB 800MHZ, Socket LGA775, Hyper-Threading, xD-bit, EM64T, VT.
2. Memory DDR SDRAM 512 PC 3200.
3. HDD 40 GB 7200 RPM.
4. VGA GeForce FX5500, 128 MB DDR DDRAM, AGP *X
5. Monitor Samsung.

3.1.2 Perangkat lunak

Perangkat lunak yang dipakai di UBP Saguling, diantaranya :

1. Sistem Operasi Windows XP professional, Windows Server 2003, Windows Server 2003
2. Microsoft Office 2003, Microsoft Office 2007
3. Trend Micro
4. Dan perangkat lunak yang dibutuhkan setiap bagian.
   a. Untuk Perangkat lunak Komputer Server

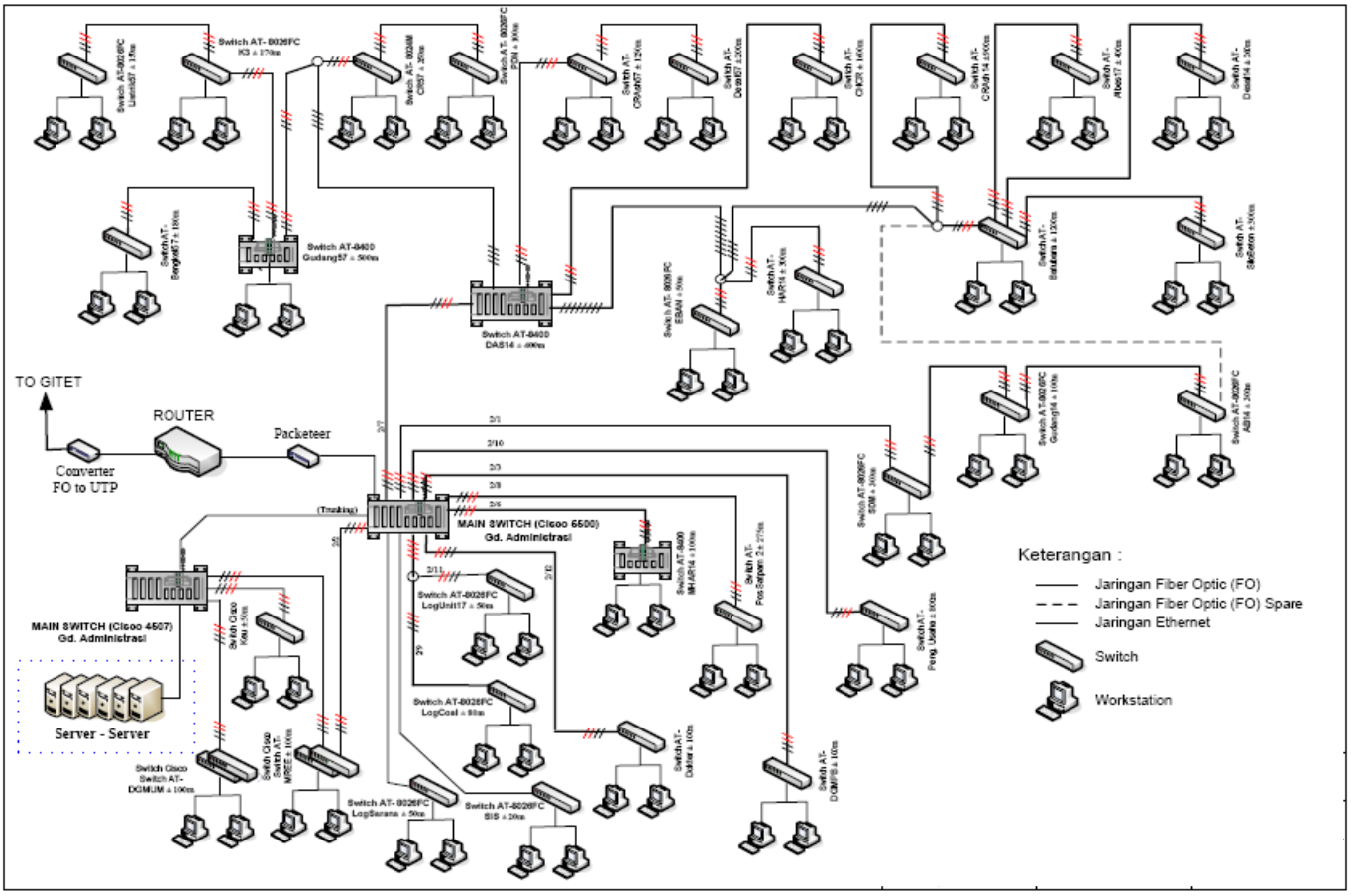
      Pada Server Sistem Operasi yang digunakan adalah Windows Server 2003.

   b. Untuk Perangkat lunak Komputer

      Pada komputer menggunakan sistem operasi yang sama yaitu Windows XP Profesional SP2. Dan package program dan ada beberapa aplikasi dan database. Contoh aplikasi yang digunakan oleh UBP Saguling adalah : Office 2003, MAXIMO, Power builder, Crystalreport, dan lain-lain. Sedangkan database menggunakan Oracle.

3.1.3 Topologi Jaringan UBP Saguling

Pada Topologi Jaringan LAN UBP. Saguling sebagai berikut :



Gambar 3.8 Topologi jaringan UBP Saguling

Topologi jaringan yang dipakai pada UBP Saguling yang terlihat pada gambar 3.8 adalah topologi star. Sistem jaringan komputer pada PT Indonesia Power tersebar di beberapa unit pembangkit diantaranya di unit bisnis pembangkit Saguling, untuk terhubung dengan jaringan unit yang lainnya harus melewati jalur yang menjadi jembatan antar jaringan unit pembangkit yaitu ICON*plus*. Dimana ICON*plus* adalah anak dari perusahaan PLN yang memberikan layanan jaringan pada unit – unit bisnis pembangkit PT Indonesia Power.

Jaringan komputer pada PT Indonesia Power merupakan jaringan kompleks yang menyediakan layanan aplikasi dan web dimana server hanya sebagai penyedia layanan bagi semua user dan tidak membatasi dan mengawasi user yang terhubung dengannya sebagaimana dengan sistem *Domain Controller*. Pada intinya jaringan PT Indonesia Power dibuat untuk mempermudah dalam hal pengumpulan data, *Sharing* data dan *Internet* serta Informasi lainnya secara *online*.

Jaringan pada PT Indonesia Power UBP Saguling merupakan jaringan LAN (Local *Area Network*) yang tersebar digedung-gedung di kawasan atau lingkungan PT Indonesia Power UBP Saguling yang sangat luas, hanya memakai satu router untuk terhubung ke kantor pusat dan jaringan ini menghubungkan UBP Saguling ke Kantor Pusat PT Indonesia Power.

Dalam koneksinya ke komputer *client* terdapat 2 tipe koneksi:

1. Jaringan Kantor Pusat

Pada jalur ini jaringan local tehubung ke jaringan kantor pusat melalui satu jalur yaitu ICON*plus* dengan kecepatan 2 Mbps. Jika UBP Saguling ingin berhubungan dengan pihak luar maka harus melalui jaringan kantor pusat dahulu, baru kemudian dapat terhubung ke luar.

2. Kabel

Pada jalur ini jaringan kabel local terhubung menggunakn kabel UTP dan FO. Untuk UTP, Koneksi ini digunakan karena dilihat dari jarak unit ke unit gedung berdekatan maka jalur koneksi menggunakan kabel UTP, sedangkan untuk koneksi untuk gedung ke gedung karna dilihat dari jaraknya yang cukup jauh maka digunakan koneksi menggunakan kabel FO.

Pada jaringan UBP Saguling kelas IP yang digunakan adalah kelas C dengan 3 segment dikarnakan banyaknya *workstation* dan peralatan memakai IP*adrees* agar terbaca pada jaringan yaitu:

192.168.21.1 - 255

192.168.101.1 - 255

192.168.201.1 – 255

3.1.4 Masalah – masalah yang sering dihadapi

Setelah menganalisa dari segi perangkat keras tidak ada masalah, dan untuk topologi tidak ada masalah, dan segi perangkat lunak juga tidak ada masalah, akan tetapi terkadang sering terjadi masalah dalam hal PC tidak terkoneksi ke jaringan. Setelah penulis melakukan praktek langsung ke lapangan, penulis yang didampingi pembimbing sering menemukan dan mendapatkan masalah yang sama, yaitu:

1. PC tidak terkoneksi ke jaringan disebabkan *deface* jaringan rusak.
   Hal ini terkadang terjadi dikarnakan *deface* jaringan terkadang rusak maka menjadi masalah dalam koneksi ke jaringan.
2. PC tidak terkoneksi ke jaringan disebabkan terinfeksi virus jaringan.
   PC tidak terkoneksi ke jaringan sering dihadapi pada setiap , lebih banyak disebabkan oleh virus jaringan. Dikarenakan masih awam menggunakan komputer dan biasanya untuk menyimpan data menggunakan *flashdisk* yang mana media tersebut rentan terinveksi virus, si hanya ngklik-klik saja yang ada pada data mereka tanpa tahu itu sudah terinfeksi oleh virus. Virus Worm Win32/Conficker.A sering menyerang komputer client di jaringan yang memiliki celah keamanan RPC Dcom 3 yang belum di-patch. Jika berhasil, maka akan terdownload *file* virus ke komputer korban. Conficker dapat melumpuhkan *System Restore* dengan cara me*reset* "Restore Point" guna mencegah korbannya membasmi virus ini dengan mengembalikan *Restore Point*. Virus ini juga akan menyebabkan matinya Internet *connection sharing*.

   Gejala Conficker yang paling umum adalah munculnya pesan *Generic Host Process Error* setiap kali pengguna komputer menghubungkan dirinya dengan internet. Selain itu, Conficker juga diketahui menyebabkan login *username Active Directory* dikunci karena ia melakukan aksi *Bruteforce*.

3.1.5 Pemecahan Masalah

1. PC tidak terkoneksi ke jaringan disebabkan *deface* jaringan rusak.

   Untuk mengetahuinya yaitu :

   a. *Pertama* dilihat kabelnya terlebih dahulu dicek menggunakan *LAN Tester*,
   b. Apabila keadaan kabel baik maka yang *kedua* adalah melihat lancard pada PC,
   c. Apabila sudah dicek dan keadaan *LAN Card* baik maka yang *ketiga* adalah melihat dari switch lalu dicek tiap port switch tersebut. Jika salah satu *deface* rusak maka akan diganti dengan *deface* yang lebih baik.

2. PC tidak terkoneksi ke jaringan disebabkan terinfeksi virus jaringan.

   Jika sudah dipastikan keadaan pada port baik, maka kemungkinan yang terjadi adalah serangan virus yang masuk ke dalam PC dan merusak sistem seperti menghilangkan salah satu *file* dalam sistem32 didalamnya, Serangan virus ini yang sering terjadi pada UBP Saguling, maka untuk mendapatkan data yang ada dalam komputer agar tidak hilang kendala ini dapat diatasi dengan cara:

   a. Cara 1.
      1. Terlebih dahulu masuk kedalam windows *safemode* lalu scan virus dengan antivirus yang ter-*up to date*.
      2. Jika sudah bersih terhadap virus, untuk menghindari terjadinya kehilangan data, maka data pada PC di backup dengan menggunakan Program *backup* Media sebelum dilakukan *repair* windows,
      3. Sesudah di *Backup* maka windows di*repair* ulang untuk me*repair* file yang hilang atau *corrupt*,
      4. Jika ada aplikasi yang *corrupt* maka harus diinstal ulang kembali.
      5. Apabila data yang telah di*backup* itu hilang karena proses *repair* maka tinggal di*restore* ulang dari *backup* yang telah dilakukan tadi.
   b. Cara 2.
      1. Dilakukan apabila cara 1 tidak dapat dilakukan (windows tidak membuka baik normal maupun *safemode*),

2. Lepas Hardisk, kemudian pasang di PC lain sebagai *slave*, kemudian lakukan *cleaning virus(scan),*
3. Lakukan sama seperti cara diatas (cara 1).

Jika antivirus pun masih gagal mengatasi, masih ada cara membasminya meski butuh sedikit kerja keras. Langkah-langkah membasmi virus Conficker dari Vaksincom berikut ini:

1. Putuskan komputer yang akan dibersihkan dari jaringan/internet. Matikan akses WiFi kalau ada dan cabut kabel ethernet dari jaringan LAN.
2. Matikan system restore (Windows XP/Vista). Caranya pilih Start>>All Program>>Accesories>>System Tools>>System Restore kemudian pada menu setting pilih off untuk seluruh partisi.
3. Matikan proses virus yang aktif pada services. Gunakan removal tool dari Norman untuk membersihkan virus yang aktif. Program ini tersedia dan dapat di*download* di http://norman.com/support/support_tools/58732/en-us
4. Delete service svchost.exe gadungan yang ditanamkan virus pada registry. Dapat dicari secara manual pada registry.
5. Hapus Schedule Task yang dibuat oleh virus. (C:-WINDOWS-Tasks)
6. Hapus string registry yang dibuat oleh virus. Untuk mempermudah dapat menggunakan script registry di bawah ini. Salin script ini lalu install.

```
[Version]

Signature=”$Chicago$”

Provider=Vaksincom Oyee

[DefaultInstall]

AddReg=UnhookRegKey

DelReg=del

[UnhookRegKey]
```

```
HKCU, Software-Microsoft-Windows-CurrentVersion-Explorer-
Advanced, Hidden, 0×00000001,1

HKCU, Software-Microsoft-Windows-CurrentVersion-Explorer-
Advanced, SuperHidden, 0×00000001,1

HKLM, SOFTWARE-Microsoft-Windows-CurrentVersion-Explorer-
Advanced-Folder-Hidden-SHOWALL, CheckedValue,
0×00000001,1

HKLM, SYSTEM-CurrentControlSet-Services-BITS, Start,
0×00000002,2

HKLM, SYSTEM-CurrentControlSet-Services-ERSvc, Start,
0×00000002,2

HKLM, SYSTEM-CurrentControlSet-Services-wscsvc, Start,
0×00000002,2

HKLM, SYSTEM-CurrentControlSet-Services-wuauserv, Start,
0×00000002,2

[del]

HKCU, Software-Microsoft-Windows-CurrentVersion-Applets,
dl

HKCU, Software-Microsoft-Windows-CurrentVersion-Applets,
ds

HKLM, SOFTWARE-Microsoft-Windows-CurrentVersion-Applets,
dl

HKLM, SOFTWARE-Microsoft-Windows-CurrentVersion-Applets,
ds

HKLM, SYSTEM-CurrentControlSet-Services-Tcpip-Parameters,
TcpNumConnections
```

Gunakan notepad untuk menyalin, kemudian simpan dengan nama “repair.inf” (gunakan pilihan Save As Type menjadi All Files agar

tidak terjadi kesalahan). Jalankan repair.inf dengan klik kanan, kemudian pilih install.

Catatan : Untuk file yang aktif pada startup, dapat men-*disable* melalui "msconfig" atau dapat men-*delete* secara manual pada string :

"HKLM, SOFTWARE-Microsoft-Windows-CurrentVersion-Run"

7. Untuk pembersihan virus W32/Conficker.DV secara optimal dan mencegah infeksi ulang, sebaiknya menggunakan antivirus yang ter-update dan mampu mendeteksi virus ini dengan baik dan patch computer dengan http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx guna mencegah infeksi ulang.

Untuk mencegah virus ini menginfeksi lebih banyak komputer lakukan langkah berikut ini:

1. Pastikan virus tersebut tidak aktif di komputer. Caranya adalah dengan memutuskan hubungan komputer ke jaringan.
2. Jika setelah hubungan ke jaringan diputuskan infeksi virus terhenti, maka artinya sumber virus bukan dari komputer melainkan dari salah satu komputer di jaringan.
3. Cari sumber penyebar virus Conficker di jaringan sebelum mengkoneksikan komputer. Logikanya, semua komputer yang belum di-patch dan terhubung ke jaringan dimana ada satu komputer yang terinfeksi virus Conficker, maka akan terinfeksi Conficker juga dalam waktu singkat. Kecuali komputer-komputer tersebut dilindungi oleh Firewall yang memproteksi port:

    1. UDP Port 135, 137, 138 dan 445
    2. TCP Port 135, 139, 445 dan 593

4. Patch semua komputer yang sistem operasinya rentan terhadap celah keamanan RPC Dcom 3. Untuk mendapatkan detil *patch*-nya, dapat di*download* di situs Microsoft.